Approved: T.H.Q
TIMOTHY T. HOWARD
Assistant United States Attorney

Before: HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

14 MAG 2427

UNITED STATES OF AMERICA - v. - BLAKE BENTHALL, a/k/a "Defcon," Defendant.	SEALED COMPLAINT Violations of 21 U.S.C. § 846; 18 U.S.C. §§ 1028, 1030 & 1956 COUNTY OF OFFENSE: NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

Vincent D. D'Agostino, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Narcotics Trafficking Conspiracy)

1. From in or about November 2013, up to and including in or about October 2014, in the Southern District of New York and elsewhere, BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to violate the narcotics laws of the United States.

2. It was a part and an object of the conspiracy that BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, would and did distribute and possess with the intent to distribute controlled substances, and aid and abet such activity, in violation of Title 21, United States Code, Section 841(a)(1).

3. It was further a part and an object of the conspiracy that BLAKE BENTHALL, a/k/a "Defcon," and others known and unknown, would and did deliver, distribute, and dispense controlled substances by means of the Internet, in a manner not

authorized by law, and aid and abet such activity, in violation of Title 21, United States Code, Section 841(h).

4. The controlled substances that BLAKE BENTHALL, a/k/a "Defcon," the defendant, conspired to distribute and possess with the intent to distribute, and to deliver, distribute, and dispense by means of the Internet, in a manner not authorized by law, and to aid and abet such activity, included, among others, 1 kilogram and more of mixtures and substances containing a detectable amount of heroin, 5 kilograms and more of mixtures and substances containing a detectable amount of cocaine, and 10 grams and more of mixtures and substances containing a detectable amount of lysergic acid diethylamide (LSD), in violation of Title 21, United States Code, Sections 812, 841(a)(1), and 841(b)(1)(A).

Overt Acts

5. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From in or about December 2013, up to and including in or about October 2014, BLAKE BENTHALL, a/k/a "Defcon," the defendant, owned and operated an underground website, known as "Silk Road 2.0," that provided a platform for drug dealers around the world to sell a wide variety of controlled substances via the Internet.

b. On or about July 30, 2014, BENTHALL transferred the Silk Road 2.0 website to a different server, in order to conceal its location and to hide it from law enforcement.

(Title 21, United States Code, Section 846.)

COUNT TWO

(Conspiracy to Commit and Aid and Abet Computer Hacking)

6. From in or about November 2013, up to and including in or about October 2014, in the Southern District of New York and elsewhere, BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to commit computer hacking offenses, and to aid and abet the same, in violation of Title 18, United States Code, Sections 1030(a)(2) and 2.

7. It was a part and an object of the conspiracy that BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, would and did intentionally access computers without authorization, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States, and would and did aid and abet such unauthorized access, in violation of Title 18, United States Code, Sections 1030(a)(2) and 2.

Overt Act

8. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt act, among others, was committed in the Southern District of New York and elsewhere:

a. From in or about December 2013, up to and including in or about October 2014, BLAKE BENTHALL, a/k/a "Defcon," the defendant, owned and operated an underground website, known as "Silk Road 2.0," that provided a platform for the sale of illicit goods and services, including malicious software designed for computer hacking, such as password stealers, keyloggers, remote access tools, and computer-hacking services.

(Title 18, United States Code, Section 1030(b).)

COUNT THREE
(Conspiracy to Transfer Fraudulent Identification Documents)

9. From in or about November 2013, up to and including in or about October 2014, in the Southern District of New York and elsewhere, BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to transfer fraudulent identification documents, and to aid and abet the same, in violation of Title 18, United States Code, Sections 1028(a)(2).

10. It was a part and an object of the conspiracy that BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, would and did knowingly transfer, in and affecting interstate and foreign commerce, and in the mail, false identification documents and authentication features, knowing

that such documents and features were produced without lawful authority, including driver's licenses, personal identification cards, and documents that appeared to be issued by and under the authority of the United States, and would and did aid and abet such transfers, in violation of Title 18, United States Code, Sections 1028(a)(2) and 2.

Overt Act

11. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt act, among others, was committed in the Southern District of New York and elsewhere:

a. From in or about December 2013, up to and including in or about October 2014, BLAKE BENTHALL, a/k/a "Defcon," the defendant, owned and operated an underground website, known as "Silk Road 2.0," that provided a platform for the sale of illicit goods and services, including fraudulent identification documents, such as fake driver's licenses and passports.

(Title 18, United States Code, Section 1028(f).)

COUNT FOUR
(Money Laundering Conspiracy)

12. From in or about November 2013, up to and including in or about October 2014, in the Southern District of New York and elsewhere, BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to commit money laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

13. It was a part and an object of the conspiracy that BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, in offenses involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions represented proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions, which in fact involved the proceeds of specified unlawful activity, to wit, narcotics trafficking, identification document fraud, and computer hacking, in violation of Title 21, United States Code, Section 841, and Title 18, United States Code, Sections 1028 and 1030,

respectively, with the intent to promote the carrying on of such specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i).

14. It was further a part and an object of the conspiracy that BLAKE BENTHALL, a/k/a "Defcon," the defendant, and others known and unknown, in offenses involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions represented proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions, which in fact involved the proceeds of specified unlawful activity, to wit, narcotics trafficking, identification document fraud, and computer hacking, in violation of Title 21, United States Code, Section 841, and Title 18, United States Code, Sections 1028 and 1030, respectively, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

Overt Acts

15. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From in or about December 2013, up to and including in or about October 2014, BLAKE BENTHALL, a/k/a "Defcon," the defendant, owned and operated an underground website, known as "Silk Road 2.0," that provided a platform for the sale of controlled substances, malicious software, and fraudulent identification documents, among other illicit goods and services, and laundered the proceeds from such sales, through the use of a payment system based on Bitcoins, an anonymous form of digital currency.

b. From in or about December 2013, up to and including in or about October 2014, BENTHALL operated a Bitcoin "tumbler" as part of the Silk Road 2.0 payment system to further ensure that illegal transactions conducted on the site could not be traced to individual users.

(Title 18, United States Code, Section 1956(h).)

* * *

The bases for my knowledge and for the foregoing charges are, in part, as follows:

16. I have been a Special Agent with the FBI for approximately ten years. I am currently assigned to a cybercrime squad within the FBI's New York Field Office. I have been personally involved in this investigation, which was conducted jointly by the FBI and Homeland Security Investigations ("HSI") with assistance from the Drug Enforcement Administration's New York Organized Crime Drug Enforcement Strike Force. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

17. As part of the investigation an HSI agent acting in an undercover capacity (the "HSI-UC") successfully infiltrated the support staff involved in running the Silk Road 2.0 website and was provided access to private areas of the website available only to BLAKE BENTHALL, a/k/a "Defcon," the defendant, and his administrative staff. In that role, the HSI-UC regularly interacted directly with BLAKE BENTHALL, a/k/a "Defcon," the defendant. Except where otherwise indicated, all references in this Complaint to communications involving "Defcon" and other co-conspirators were obtained by the HSI-UC through his undercover access to Silk Road 2.0. I have reviewed screenshots taken by the HSI-UC that document all the referenced communications.

OVERVIEW

18. Since in or about December 2013, BLAKE BENTHALL, a/k/a "Defcon," the defendant, has secretly owned and operated an underground website known as "Silk Road 2.0" - one of the most extensive, sophisticated, and widely-used criminal marketplaces on the Internet today. Since its launch in November 2013, Silk Road 2.0 has been used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to over a hundred thousand buyers throughout the world, as well as to launder tens of millions of dollars generated by these unlawful transactions.

As of October 2014, Silk Road 2.0 was generating sales of at least approximately $8 million in United States currency per month.

19. Silk Road 2.0 was created in the wake of the Government's seizure in October 2013 of the website known as "Silk Road" (hereinafter "Silk Road 1.0") and the arrest of its alleged owner and operator, Ross William Ulbricht, a/k/a "Dread Pirate Roberts." Silk Road 1.0 had been designed to enable users anywhere in the world to buy and sell illegal drugs and other illegal goods and services anonymously and beyond the reach of law enforcement. Before its seizure in October 2013, Silk Road 1.0 was used extensively to facilitate such transactions.

20. On or about November 6, 2013, several weeks after the Government shut down Silk Road 1.0 and arrested Ulbricht, Silk Road 2.0 was launched. Silk Road 2.0 was specifically designed to fill the void left by the Government's seizure of Silk Road 1.0 and was virtually identical to Silk Road 1.0 in its appearance and function. In particular, like its predecessor, Silk Road 2.0 operated exclusively on the "Tor" network,[1] and required all transactions to be paid for in Bitcoins,[2] in order to preserve its users' anonymity and evade detection by law enforcement.

21. Silk Road 2.0 initially was owned and operated by another individual (hereinafter referred to as "DPR2") who adopted the online pseudonym "Dread Pirate Roberts," which allegedly had been used previously by Ross Ulbricht. Then, on

---

[1] The Tor network ("Tor") is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion."

[2] Bitcoins are an anonymous, decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. Bitcoins are not illegal in and of themselves and have known legitimate uses. However, Bitcoins are also known to be used by cybercriminals for money-laundering purposes, given the ease with which they can be used to move money anonymously.

or about December 20, 2013, BLAKE BENTHALL, a/k/a "Defcon," the defendant, who had been acting as second-in-command to DPR2, assumed control of Silk Road 2.0 and has owned and operated the site continuously since that time. BENTHALL has controlled and overseen all aspects of Silk Road 2.0, including, among other things: the computer infrastructure and programming code underlying the website; the terms of service and commission rates imposed on vendors and customers of the website; the small staff of online administrators and forum moderators who have assisted with the day-to-day operation of the website; and the massive profits generated from the operation of the business.

BACKGROUND OF THE SILK ROAD 2.0 WEBSITE

Launch of Silk Road 2.0

22. On or about November 6, 2013, approximately five weeks after Ulbricht was arrested and Silk Road 1.0 was shut down by the Government, a successor website calling itself "Silk Road 2.0" emerged on the Tor network. The website clearly marketed itself as the successor to Silk Road 1.0. For example:

a. I have reviewed screenshots reflecting that, as of approximately November 6, 2013, the Silk Road 2.0 marketplace was accessible from a Tor address which included an explicit reference to Silk Road ("http://silkroad6ownowfk.onion").

b. I have reviewed screenshots of the original login page for Silk Road 2.0, as it appeared on or about November 6, 2013. The login page contained as its background an altered image of the seizure banner that the Government had placed on the Silk Road 1.0 website. Whereas the original seizure banner read "THIS HIDDEN SITE HAS BEEN SEIZED," the altered image of the seizure notice on the Silk Road 2.0 login page read: "THIS HIDDEN SITE HAS RISEN AGAIN." A screenshot of the Silk Road 2.0 login page as it existed at the site's inception is attached hereto as Exhibit A.

c. Upon logging into the site, a user received a welcome message from the new administrator who, like the owner and operator of Silk Road 1.0, used the online pseudonym "Dread Pirate Roberts."[3] The welcome message announced that:

[3] "Dread Pirate Roberts" is a reference to a fictional character in the 1987 motion picture The Princess Bride. Based on my familiarity with the film, I know that the film portrays the legend of the "Dread Pirate Roberts" character as bearing a name not belonging a single individual, but belonging to a series of

> It is with great joy that I announce the next chapter of our journey. Silk Road has risen from the ashes, and is now ready and waiting for you all to return home.

Design of the Site

23. Throughout the investigation, I, and other law enforcement agents, including the HSI-UC, have visited Silk Road 2.0 using undercover user accounts. From reviewing the content of the website, I know that the site is designed in the same manner as Silk Road 1.0 and serves the same basic illegal function, providing an anonymous online platform for the large-scale distribution of controlled substances, computer hacking tools and services, fraudulent identification documents, and other contraband. For example:

a. The appearance of the site is almost identical to that of Silk Road 1.0, including the same distinctive green logo, consisting of a nomad on a camel.

b. Silk Road 2.0 offers its users an almost identical user experience to that offered on Silk Road 1.0.[4] Specifically, Silk Road 2.0 is accessed through Tor browser software at its ".onion" address, where users log onto the site using a username and password.[5] The website contains a user-friendly interface with links to various categories of items for sale on the site, which include, most prominently, "Drugs," within which are sub-categories of various types of narcotics. Clicking on any of the links to items for sale on the site brings up a webpage containing the details of the listing, including a description of the item, the price, the username of

---

individuals, each of whom passes his name and reputation to a chosen successor.

[4] The design and functionality of the Silk Road 1.0 website are set forth in detail in paragraphs 18(c) through 18(p) of the complaint filed in the United States District Court for the Southern District of New York in United States v. Ross Ulbricht, 13 Mag. 2328.

[5] New users have the option of setting up a new account, and can select their own unique username and password. Users are not required to input any identification information, and the user is not subject to any verification.

the vendor selling the item, and prior customers' "feedback" on the vendor's "product." To buy an item listed, the user can simply click the link labeled "add to cart." The user is then prompted to supply a shipping address and to confirm the placement of the order. Once the order is placed, it is processed through Silk Road 2.0's Bitcoin-based payment system, described further below.

c. Silk Road 2.0 contains a number of additional communication services for its users that were also available on Silk Road 1.0. These include: (1) a private message system, which allows users to send messages to one another through the site, similar to emails; (2) a customer support page, where users can obtain help with using the website from administrators; and (3) online forums, overseen by forum moderators, where users can post and comment on topics relating to the website.

d. Like its predecessor, Silk Road 2.0 also includes its own Bitcoin-based payment system designed to facilitate payments from users to vendors while concealing the identities of the parties involved in the unlawful transactions. In order to make purchases on the site, a user must first obtain Bitcoins (typically from a Bitcoin exchanger) and transfer them to the user's Silk Road 2.0 account. The user can then make purchases from vendors, who receive credit for the user's payments in their Silk Road 2.0 accounts. Vendors and users can withdraw Bitcoins from their Bitcoin balances at any time, by providing Silk Road 2.0 with an independent Bitcoin address,[6] outside the control of Silk Road 2.0, where the Bitcoins should be sent. At no point in the process is the user or vendor required to provide any identifying information to Silk Road 2.0 to move funds through the site.

e. Like Silk Road 1.0, Silk Road 2.0 uses a so-called "tumbler" (also referred to as a "mixer") to process Bitcoin transactions. Based on my training and experience, I know that such "tumblers" are designed to frustrate the tracking of individual Bitcoin transactions, by passing the Bitcoins through numerous dummy transactions on the Blockchain - a public ledger where all Bitcoin transactions are recorded. The "tumbler" thereby obscures any link between the Bitcoin addresses involved in Silk Road 2.0 transactions - making it fruitless to use the Blockchain to follow the money trail

[6] A Bitcoin "address" is the term for an account on the Bitcoin network, where Bitcoins may be stored.

involved in the transaction, even if the buyer's and vendor's Bitcoin addresses are both known. Based on my training and experience, such "tumblers" are commonly used to assist with the laundering of criminal proceeds.

f. Finally, as with Silk Road 1.0, Silk Road 2.0 charges a commission for every transaction conducted by its users. At times, there has been a flat rate on all transactions. At other times, the rate has varied depending on the size of the sale, but generally has ranged from four to eight percent.

Illegal Goods and Services Sold on the Site

24. On or about October 29, 2014, I accessed Silk Road 2.0 from an undercover user account, from a computer located in the Southern District of New York. I observed that the Silk Road 2.0 marketplace was dominated by offerings for illegal narcotics, with 14,024 different listings offering the sale of "Drugs," including, among others, 1,654 listings for "Psychedelics," 1,921 listings for "Ecstasy," 1,816 listings for "Cannabis," and 360 listings for "Opioids." A screenshot of the Silk Road 2.0 homepage as it appeared during this observation, depicting product listings by category, is attached hereto as Exhibit B.

25. On or about September 14, 2014, the HSI-UC captured screenshots of a portion of the thousands of illegal products and services that were available for sale on Silk Road 2.0 at the time. Those products included, among other things:

a. Heroin: A listing for 100 grams of "Afghan Heroin Brown Powder" for approximately 9.70 Bitcoins, the equivalent of approximately $4,555 in United States currency, based on the prevailing exchange rate that day.[7]

b. Cocaine: A listing for 5 grams of "Highest Purity Cocaine - Direct From Colombia" available for shipment from the United States to any location in the world. The

[7] In addition, on or about October 17, 2014, I accessed Silk Road 2.0 from an undercover account and captured a screenshot of a listing offering 1 gram of heroin ("1g #3 Afghan Heroin High Quality Uncut Pure From the Brick") for 0.123 Bitcoins, the equivalent of approximately $47 in United States currency, based on the prevailing exchange rate that day. A screenshot of that listing is attached hereto as Exhibit C.

listing advertised the sale of the narcotics for 1.04 Bitcoins, the equivalent of approximately $488 in United States currency, based on the prevailing exchange rate that day.

c. Fake Danish Passport: A listing for a fraudulent Danish passport, with "all the security features and original pages" of a "real Danish Passport," priced at 5.14 Bitcoins, the equivalent of approximately $2,414 in United States currency, based on the prevailing exchange rate that day.

d. Fake New Jersey Driver's License: A listing for a fraudulent New Jersey driver's license, including holograms, for 0.21 Bitcoins, the equivalent of $98 in United States currency, based on the prevailing exchange rate that day.

e. Website Hacking Services: A listing offering a service "to HACK the website you want," noting that after the service is purchased, the seller would "invest 4-7 days into hacking the account." The fee for the service was advertised as 1.32 Bitcoins, the equivalent of approximately $624 in United States currency, based on the prevailing exchange rate that day, and noted that "[h]alf the money will be paid before beginning and half after and if I get the password."

f. Email Hacking: A listing offering to sell a method for hacking Gmail email accounts, for 0.09 Bitcoins, the equivalent of approximately $42 in United States currency, based on the prevailing exchange rate that day.

26. As part of the investigation, law enforcement agents with the DEA have made multiple undercover purchases of illegal narcotics from Silk Road 2.0. For example, based on reports prepared by a DEA agent, I have learned that, in or about September and October 2014, the DEA purchased the following controlled substances on Silk Road 2.0: (1) 0.5 grams of heroin; (2) two grams of cocaine; (3) 120 micrograms of lysergic acid diethylamide (commonly referred to as "LSD"); and (4) ten 30-milligram pills of oxycodone. Each of these substances was sent to and received by the DEA at an undercover address located in Manhattan, and each field-tested positive for the presence of the controlled substance that had been ordered from Silk Road 2.0.

THE ROLE OF "DEFCON" ON SILK ROAD 2.0

Assumption of Control in December 2013

27. As set forth in detail below, based on my discussions with the HSI-UC, as well as my review of public posts on Silk Road 2.0 and private communications to which the HSI-UC had access, Silk Road 2.0 was initially launched in November 2013 by DPR2, but Defcon soon took over the operation of the site approximately six weeks later in December 2013, and has remained in control ever since.

28. Between on or about October 7, 2013 and on or about November 6, 2013, DPR2 took various steps to launch the Silk Road 2.0 underground market:

a. On or about October 7, 2013, the HSI-UC was invited to join a newly created discussion forum on the Tor network, concerning the potential creation of a replacement for the Silk Road 1.0 website. The next day, on or about October 8, 2013, the persons operating the forum gave the HSI-UC moderator privileges, enabling the HSI-UC to access areas of the forum available only to forum staff. The forum would later become the discussion forum associated with the Silk Road 2.0 website (the "SR2 Forum").

b. On or about October 7, 2013, DPR2 posted a message to the SR2 Forum directed to prior vendors from Silk Road 1.0, inviting them to participate as vendors on the planned Silk Road 2.0 website: "To all former Silk Road vendors, we will be providing you free vendor accounts on the new marketplace, I do not believe you should have to pay again for the privilege of selling if you are already established and I further recognise the losses many of you unfortunately made during the seizure of the original site."[8]

c. On or about October 8, 2013, DPR2 posted a message to the SR2 Forum stating, in sum and substance, that he was not the same "Dread Pirate Roberts" who ran Silk Road 1.0 and that he had "taken steps the previous Dread Pirate Roberts wouldn't have even thought of" to protect the servers that would run the new website.

[8] The online communications quoted in this affidavit are included in substantially verbatim form; punctuation and grammatical errors have not been corrected.

29. As noted above, the Silk Road 2.0 marketplace was launched on or about November 6, 2013. Within approximately a week of the launch, the HSI-UC observed an individual using the moniker "Defcon" emerge as an administrator on the SR2 Forum. On or about November 13, 2013, Defcon posted a message to the SR2 Forum stating: "Just wanted to check in with you all and say hi to the community. I won't be around on public forums often. . . . DPR has asked I don't discuss my role at all with you but that is probably in the better interests of us all." Later that day, DPR2 responded by posting a message stating: "Welcome to the team, Defcon, it is always good to see fresh (metaphorical) faces."

30. On or about December 20, 2013, the United States Attorney's Office for the Southern District of New York announced the arrests of three alleged administrators of Silk Road 1.0 - Andrew Michael Jones, a/k/a "Inigo," Gary Davis, a/k/a "Libertas," and Peter Phillip Nash, a/k/a "Samesamebutdifferent," a/k/a "Batman73," a/k/a "Symmetry," a/k/a "Anonymousasshit". Following this announcement, and the ensuing discussion of the arrests in the media and on the SR2 Forum, DPR2 abandoned his role as operator of Silk Road 2.0, and Defcon took his place. Specifically:

a. On or about December 20, 2013, Defcon posted a message to the SR2 Forum stating: "Three of our dear friends were arrested in connection to their SR1.0 activities. They did not have access to anything which would compromise the marketplace. We are watching everything very closely regardless."

b. On or about December 22, 2013, Defcon posted a message to the SR2 Forum concerning DPR2's reaction to the news of the arrests: "The Captain is alive and well and is in touch with key staff members. I cannot reveal much, but here are the key facts: DPR places operational security above all else, including posting updates to this forum. Given his role he has every right to play it very safe."

c. Later that day, Defcon posted another message on to the S2 Forum concerning DPR2's absence from the site, in which he also noted that he was second-in-command to DPR2: "It has been over 24 hours since we last heard from our Captain. He is most certainly in grave danger. . . . As his second in command, I have very clear instructions as to what to do in this worst case scenario. . . I cannot elaborate on the specifics,

but the marketplace is safe in my hands until the Captain returns or his successor appears."

d. On or about December 28, 2013, Defcon posted a message to the SR2 Forum, announcing that he had taken over control of the Silk Road 2.0 marketplace and would reopen it later that day. Among other things, Defcon wrote: "Merely three months have pass since our marketplace's first incantation was captured by our oppressors. This was a brutal blow, but we are very proud that such a devastating compromise only resulted in one month of downtime. . . . I intend to prove to you that leading this movement forward is my top priority in life, and that I will pour any time and energy necessary into ensuring its success. . . While other admins may run away when calamities strike - I'm ready to fight right here alongside you."

Management of the Silk Road 2.0 Infrastructure

31. Since assuming control of Silk Road 2.0 as of late December 2013, Defcon has controlled virtually every aspect of Silk Road's operation. First, Defcon has been responsible for the Silk Road 2.0 infrastructure, including managing its servers and making improvements to the site to better protect users' anonymity, among other purposes. For example:

a. Defcon has been responsible for maintaining and upgrading the Bitcoin-based payment system on Silk Road 2.0. For example, on or about April 7, 2014, Defcon publicly announced the unveiling of "upgraded Bitcoin infrastructure" on Silk Road 2.0, which included "[e]xponentially faster deposit and withdrawal times," and "[i]ncreased server anonymity." Similarly, on or about May 8, 2014, Defcon announced further efforts "to expand our Bitcoin infrastructure's ability to process more cash deposits per minute while preserving server anonymity and security." On both of these occasions, the HSI-UC observed corresponding changes to the website's Bitcoin-based payment system following these announcements.

b. Defcon was also responsible for changing the servers hosting Silk Road 2.0 on or about July 30, 2014, after the Tor Project (which helps administer the Tor network) publicly announced a vulnerability in Tor that threatened to compromise the anonymity of Tor websites like Silk Road 2.0. That day, Defcon responded to a message in the SR2 Forum exclusively available to administrators and moderators, including the HSI-UC, entitled "Re: torproject say move servers." That message indicated that Defcon was arranging to

change the server hosting the Silk Road 2.0 website in light of the reported Tor vulnerability: "We are confident our unordinary servers are relatively safer than most hosting approaches, but will be moving servers again today. This is very expensive and irritating, but a necessary must. Expect a public announcement and downtime at some point over the next 24 hours. We are provisioning the replacements and not connecting to possibly compromised devices." Following this announcement, the HSI-UC observed the Silk Road 2.0 website temporarily go offline as Defcon had advised.

Control of Profits Generated by Silk Road 2.0

32. Defcon has also maintained control of the commission rates for the sale of illegal narcotics and other contraband on Silk Road 2.0. For example:

a. On or about January 14, 2014, Defcon posted a message to the SR2 Forum in which he confirmed that he was personally in control of the commission rates charged on the site, which at that time ranged from four to eight percent, based on the size of the transaction. In that message, Defcon stated that he had "the right to set the commission structure at whatever I want" and that "the current rates are fair given the extreme amount of risk on staff's shoulders." Further, Defcon stated that he believed the commission rate was justified, given the risks of arrest that he and his staff were assuming, stating: "I have no doubt that we have the highest traffic and therefore the highest LE [i.e., law enforcement] crosshairs on our foreheads . . . [p]urchases are going up, vendors are going up - and alongside this, the amount of personal risk staff is taking is exponentially going up. The bigger we become, the more resources agencies are willing to spend on hunting us."

b. On or about February 19, 2014, Defcon made an announcement on the SR2 Forum that he was setting the commission rate at five percent for all sales on Silk Road 2.0.

33. Defcon's control over the proceeds generated from Silk Road is further evidenced by other communications of Defcon observed by the HSI-UC, in which Defcon demonstrated intimate knowledge of those proceeds. Those communications indicate that, by in or about October 2014, Silk Road 2.0 was generating at least approximately $8 million in monthly sales and at least $400,000 in monthly commissions. Specifically:

a. On or about September 10, 2014 and September 11, 2014, Defcon sent a series of messages to his support staff, reporting, in sum and substance, that a computer hacker had stolen all of the Bitcoins from the Silk Road 2.0 marketplace server. Defcon's messages indicated that the stolen funds had been held on the Silk Road 2.0 server to cover user balances available for withdrawal.

b. On or about September 10, 2014, Defcon provided his support staff with the Bitcoin address where he believed the hacker had transferred the stolen funds to ("Bitcoin Address-1"). I have checked publicly available information on the Blockchain regarding Bitcoin Address-1, which indicates that, on or about September 10, 2014, hundreds of transfers were made to that address, for a total of approximately 2,987.8 Bitcoins, the equivalent of approximately $1,412,000 in United States currency based on the prevailing exchange rate that day.

c. In the immediate wake of the purported Bitcoin theft, the Silk Road 2.0 marketplace was temporarily closed.

d. On or about September 11, 2014, Defcon had an online conversation with the HSI-UC, in which he discussed, in sum and substance, his intention to reopen the Silk Road 2.0 marketplace, and his plan to recoup the deficit of Bitcoins that had been stolen from Silk Road 2.0. Specifically, Defcon confirmed that the site needed to recoup approximately 2,900 Bitcoins to cover the loss, and stated that he intended to donate approximately 1,000 of his own Bitcoins to return liquidity to Silk Road 2.0 ("I'm planning to throw my 1000 BTC to kickstart the thing."). Defcon further acknowledged that the site had approximately 150,000 monthly active users ("We have 150,000 monthly active users. That's why we have to save this thing."). The HSI-UC asked how long it would take to recover from the theft, and Defcon replied that it would take approximately three months' worth of commission payments, if sales on Silk Road 2.0 continued at a steady rate ("Three months if sales continue at current pace and we don't bottom out"). Thus, Defcon appears to have expected Silk Road 2.0 to generate approximately $6 million in monthly sales over the next three months, which would have resulted in commissions over that three-month period totaling approximately $900,000 - equal to approximately 1,900 Bitcoins at the then-prevailing exchange rate. [9]

[9] This estimate is based on the conservative assumption that Defcon was only referring to overcoming a deficit of 1,900

e. Approximately one month later, on or about October 10, 2014, Defcon posted a message to a part of the SR2 Forum exclusively available to the Silk Road 2.0 support staff, in which he indicated that the site had recouped 1,000 Bitcoins since the September 10, 2014 hack. Accordingly, it appears that the website had exceeded Defcon's expectations and generated over $400,000 in commissions and, correspondingly, over $8 million in sales, over the past month, based on the prevailing Bitcoin exchange rate from September 10 to October 10, 2014.

Management of Administrative Staff

34. According to the HSI-UC, since Defcon assumed control over Silk Road 2.0 in December 2013, he has been responsible for managing the support staff responsible for the day-to-day operations of the site. Defcon has determined the duties for which each staff member has been responsible and has controlled the level of access granted to each staff member to the administrative areas of the site. Staff members have treated Defcon as their boss and have looked to him for instruction and guidance in carrying out their roles, answering user inquiries, and resolving disputes between buyers and vendors.

35. Defcon has also been responsible for paying compensation - including salaries and bonuses - to the support staff. The HSI-UC, for example, has received regular payments from Defcon since on or about January 23, 201 - approximately 16 payments in total, amounting to approximately 83.39 Bitcoins (the equivalent of approximately $32,189 in United States currency based on current exchange rates). In addition, Defcon has regularly made posts to the section of the SR2 Forum reserved for the support staff, providing reports on the status of their salary payments.

Recruitment of Vendors

36. Defcon also coordinated attempts to recruit large-scale narcotics vendors to Silk Road 2.0. For example:

Bitcoins (subtracting the 1,000 Bitcoins he said he would donate). Given the commission rate of five percent charged on Silk Road 2.0 at the time, it would have required approximately $6 million in monthly sales over a three-month period to generate sufficient commissions to recover this amount.

a. On or about March 16, 2014, Defcon posted a message in a section of the SR2 Forum reserved for the support staff, in which he called on his staff to analyze other black-market websites, and to identify "bulk vendors and high-volume vendors," who could be recruited to Silk Road 2.0. Later in the message, Defcon included draft analyses of two other black-market websites, including descriptions of the volume of narcotics distributed on those sites.

b. On or about March 17, 2014, Defcon posted another message in the same section of the SR2 Forum, asking the staff to brainstorm as to how to "grow our vendor userbase," noting that the priority was to recruit "high volume bulk vendors." One moderator ("Moderator-1") responded to Defcon's post, indicating that they needed to focus on certain types of narcotics vendors ("We certainly do need more vendors who can run a smooth operation and offer products that are in high demand at a competitive price (Heroin, Prescription Pills, Cocaine, Bulk Cannibis)"). Another moderator ("Moderator-2") added that they should focus on the types of drug vendors mentioned by Moderator-1 who sold narcotics on Silk Road 1.0 but had not continued to participate as vendors on Silk Road 2.0 (noting that they should "attempt[] to take the ones who never came to SR2 in the first place after SR1 fell . . . [e]specially those who vend high demand products like the ones [Moderator-1] mentioned"). Defcon responded by requesting that Moderator-2 compile a list of such vendors.

Protecting Silk Road 2.0 from Law Enforcement

37. Defcon's communications also reflect that Defcon has been keenly aware of the illegal nature of the commerce being hosted on Silk Road 2.0, and that he has repeatedly taken steps to protect Silk Road 2.0, as well as its vendors and users, from law enforcement. For example:

a. On or about January 2, 2014, Defcon posted a message on the part of the SR2 Forum accessible exclusively to vendors, warning vendors located in Minnesota to exercise caution, including by destroying evidence and temporarily stopping their activities, based on intelligence he had received that the FBI was preparing for a "large darknet-related operation in Minnesota" ("Two of our informants have warned us that a large number of FBI agents have been sent to Minnesota for a large darknet-related operation. One of these informants was correct very recently, but we did not receive the information in time. . . . If you are operating in this region,

staff urges you to destroy information and go dark, or at bare minimum strengthen your operational security. Assume your home will be raided. Operate in a different location . . . .").

b. On or about January 5, 2014, Defcon posted a message in the same section of the SR2 Forum in which he bragged about Silk Road 2.0 being the largest black market website on the Internet ("We are the most major market on the darknet site at this point"). Further, Defcon urged buyers to encrypt their addresses in all purchases, to protect them from law enforcement ("We are in a position to teach an incredibly valuable life skill for this buyer community: always encrypt. . . . We are doing this more for buyers' sake than vendors' sake. PGP encryption teaches users to never enter their address on ANY darknet site, which greatly decreases LE's ability to set up honeypots.").

c. On or about January 10, 2014, Defcon posted another message in the same section of the SR2 Forum, in which he announced his "priority list" in administering Silk Road 2.0. Defcon listed his top priority as the need to conceal Silk Road 2.0 servers and protect them from seizure by law enforcement ("Prevent servers from being seized by LE . . . [T]his has been consuming most of my time and I cannot elaborate on it, nothing's in danger, but scaling a site this large requires a lot of odd approaches to server stealth.").

d. On or about May 8, 2014, Defcon sent a private message to Silk Road 2.0 staff, including the HSI-UC, in which he described updates that he recently made to the Silk Road 2.0 infrastructure, including updates to the servers that would protect sensitive information from being recovered in the event they were seized by law enforcement ("A significant infrastructure change occurred over the last week with minimal downtime. Cannot elaborate, but it increases our community's anonymity and security in the event of seizure. Dev team's design requirements are that the servers should be able to be seized and reveal nothing.").

IDENTIFICATION OF "DEFCON" AS BLAKE BENTHALL, THE DEFENDANT

38. As described in detail below, the investigation has established that the true identity of "Defcon" is BLAKE BENTHALL, a/k/a "Defcon," the defendant. Evidence recovered during the course of the investigation shows that BENTHALL personally administered the server used to host the Silk Road

2.0 website and further evidence corroborates that he is the same individual as the Silk Road 2.0 administrator known as "Defcon."

39. First, the investigation successfully located a server used to host the Silk Road 2.0 website, which, based on the contents of the server, appears to have been controlled by Defcon at the time. Specifically:

a. In or about May 2014, the FBI identified a server located in a foreign country that was believed to be hosting the Silk Road 2.0 website at the time (the "Silk Road 2.0 Server"). On or about May 30, 2014, law enforcement personnel from that country imaged the Silk Road 2.0 Server and conducted a forensic analysis of it. Based on posts made to the SR2 Forum, complaining of service outages at the time the imaging was conducted, I know that once the Silk Road 2.0 server was taken offline for imaging, the Silk Road 2.0 website went offline as well, thus confirming that the server was used to host the Silk Road 2.0 website.

b. A copy of the image of the Silk Road 2.0 server made by the foreign authorities was subsequently provided to the FBI. The data that was obtained further confirmed that the Silk Road 2.0 Server was hosting services related to Silk Road 2.0, including, among other things, the following:

i. The server included configuration files for the SR2 Forum, along with the private key required to operate the SR2 Forum as a Tor hidden service on the Internet.[10]

ii. The configuration of the server indicated that the only user account on the server was named "dpr," consistent with the "Dread Pirate Roberts" pseudonym used by DPR2 when Silk Road 2.0 was initially launched.

c. Further, the Silk Road 2.0 Server contained chat logs, reflecting conversations between DPR2 and Defcon regarding the administration of Silk Road 2.0. These chats included discussions between individuals using the online pseudonyms "myself" and "captain." As noted above in paragraphs 30(c)

[10] A server operating a Tor hidden service requires a "private key" (a cryptographic key) be resident on the server. The private key corresponds to a public key users of the servers need to communicate with the Tor hidden service.

through 30(e), Defcon repeatedly referred to DPR2 as "captain" in posts to the SR2 Forum. Based on the context provided by the chats, including their timing, as well my familiarity with this investigation, I believe that the user reflected as "myself" in the chats was "Defcon," and that he was communicating with DPR2 in the chats. For example:

i. During a chat logged on January 28, 2014, "captain" and "myself" discussed the arrest of "btcking" – an apparent reference to Robert M. Faiella, a/k/a "BTCKing," whose arrest had been announced the previous day by the United States Attorney's Office for the Southern District of New York, based on Faiella's alleged operation of an underground Bitcoin exchange service on Silk Road 1.0. During the conversation, "myself" indicated that he had deactivated the account that "btcking" had on Silk Road 2.0 ("disabled his account, changed passwords, refunded unshipped orders, removed listings"). Based on my training and experience, and my familiarity with the investigation, this conduct is consistent with Defcon's role as chief administrator of the site at the time, as it appears to have been intended to prevent law enforcement from taking control of the "btcking" account and using it to investigate the Silk Road 2.0 website or its users who were clients of "btcking."

ii. During the same January 28, 2014 chat, "captain" stated, "With every bust my retirement hastens," consistent with DPR2 seeking to complete his full withdrawal from Silk Road 2.0 because he was afraid of being arrested. The chat also included discussions about a "pension plan" for "captain," in which "myself" proposed "50/50" split in earnings for the time period "up until you left." At the end of the conversation, "captain" refers to providing "myself" with access to his private keys and accounts, and discusses the "handover." This conversation is consistent with Defcon ("myself") discussing remuneration to DPR2 ("captain") for his prior work as chief administrator of Silk Road 2.0 until late December 2013, when he departed, and DPR2 ("captain") completing the full handover of control to Defcon ("myself").

iii. Further, the server contained another chat, dated December 13, 2013, during the time that Defcon worked as second in command to DPR2. During that chat, "myself" posted a draft message to users regarding alternate .onion addresses where the Silk Road 2.0 marketplace could be accessed while the site was experiencing heavy traffic, and requested that "captain" sign the messages and add his PGP encryption key.

"Captain" responded by adding "Dread Pirate Roberts" to the messages drafted by Defcon, and adding an encryption signature. Accordingly, the timing and contents of this chat further confirm that "captain" was being used by DPR2 and "myself" was being used by Defcon during this chat.

g. Accordingly, I believe that Defcon was the party labeled as "myself" in chat logs recovered from the Silk Road 2.0 Server. Further, I know, based on my training and experience, that the default setting of many chat programs is to refer to the user of the program logging the chats as "myself." Accordingly, I submit that there is probable cause to believe that Defcon stored these chat logs on the Silk Road 2.0 Server, and that he therefore had administrative access to and control over the Silk Road 2.0 Server.

40. Based on a review of records provided by the service provider for the Silk Road 2.0 Server (the "Provider"), I have discovered that the server was controlled and maintained during the relevant time by an individual using the email account "blake@benthall.net" ("Benthall Email Account-1"). Specifically:

a. Subscriber records for the Silk Road 2.0 Server indicate that the customer leasing the server from the Provider supplied two email addresses as part of the customer's contact information, including Benthall Email Account-1.

b. Further, records obtained from the Provider indicate that it regularly sent service alerts regarding the server to Benthall Email Account-1, including on or about: November 16, 2013; January 13, 2014; February 21, 2014; February 22, 2014; February 24, 2014; February 25, 2014; March 3, 2014; May 30, 2014; and June 10, 2014.

c. Specifically, on or about May 30, 2014, the day that foreign law enforcement authorities were imaging the Silk Road 2.0 Server, the service provider sent a total of approximately 24 notifications to Benthall Email Account-1, which noted that the Silk Road 2.0 Server was offline. Following these notices, the Provider received a customer support message through its online support system, which, according to records maintained by the Provider, was submitted from a certain IP address ending with ".116" ("IP Address-1"). That customer support inquiry stated, in part: "Our server srv2.close.co has not been responding for several hours. Do NOT reboot the machine, there is a critical process we need to

watch." Based on my training and experience, I know that rebooting a computer deletes any information stored in the computer's short-term ("RAM") memory, which, depending on the configuration of the server, can include files needed to operate the website. Accordingly, I believe that in this message, the customer, after receiving notification from the Provider that the server was offline, was asking the Provider to refrain from rebooting the server in order to avoid the need for time-consuming intervention by the administrator to restart the service.

d. IP logs obtained from Google, Inc. ("Google"), the service provider for Benthall Email Account-1, indicate that, on or about May 30, 2014, the user of Benthall Email Account-1 logged into that account from IP Address-1 approximately 146 times. As noted above, IP Address-1 was used on the same date to send support requests to the Provider concerning the Silk Road 2.0 Server, further demonstrating that the user of Benthall Email Account-1 controlled and administered the Silk Road 2.0 Server.

e. Further, on or about June 10, 2014, records obtained from the Provider indicate that, during the course of the day, the Provider received multiple customer support messages through its online support system from someone using a certain IP address ending with ".6" ("IP Address-2"). The customer support messages indicated that the customer could not access the server and that the server would not finish booting. The customer further stated that the server contained "highly confidential client data covered by ITAR [international arms-trafficking] government restrictions," and the problem with the server was "extremely urgent" because the server was maintained for a "government client." As noted above, the data recovered from the Silk Road 2.0 Server indicates that the server was used to host the Silk Road 2.0 website; there is no indication that it was used to host any content relating to any "government client." Accordingly, I believe that these messages indicate that the customer reporting the service outage was aware of the illegal contents of the Silk Road 2.0 server, and that he falsely represented to the Provider that the server contained sensitive government data in order to prompt a quick response and to ensure that the Provider did not examine the (supposedly government-sensitive) contents of the server.

f. Subscriber information for IP Address-2 indicates that, on or about June 10, 2014, IP Address-2 belonged to a certain hotel in South Lake Tahoe, California ("Hotel-1"). I

have discovered that BLAKE BENTHALL, a/k/a "Defcon," the defendant, was a guest of Hotel-1 on that date, based on a review of the contents of Benthall Email Account-1, obtained through a court-authorized search warrant of the account. Accordingly, I believe that BENTHALL sent the July 10, 2014 support requests to the Provider regarding the Silk Road 2.0 Server from IP Address-2.

g. Based on information obtained from the Provider, account invoices for the Silk Road 2.0 Server were accessed on or about April 22, 2014 from an IP address belonging to a certain hotel in Las Vegas, Nevada ("Hotel-2"). Based on records provided by Hotel-2, BENTHALL was a guest at Hotel-2 on or about April 22, 2014, and Hotel-2 had Benthall Email Account-1 as the listed contact e-mail address for BENTHALL.

41. According to subscriber information provided by Google for Benthall Email Account-1, the account is registered to "Blake Benthall." I have reviewed the contents of Benthall Email Account-1, which include numerous emails in which the user identifies himself as "Blake Benthall." Notably, the account also contains an email linking the user of the account to Silk Road 2.0: specifically, the account contains an email dated November 20, 2013, which the user of the email account appears to have sent to himself, containing links to private messages viewable only by members of the SR2 Forum.

42. I have also reviewed publicly available Internet social networking profiles associated with Benthall E-Mail Account-1, which corroborate that BALKE BENTHALL, a/k/a "Defcon," the defendant, is the user of Benthall Email Account-1, and which further associate BENTHALL with Silk Road 2.0, including the following:

a. I have reviewed the publicly available profile of "Blake Benthall" on GitHub, a social networking website focused on software development, which lists Benthall Email Account-1 as the contact email address, and also includes a photograph of BENTHALL as the user. The profile also includes links to websites and discussions regarding Bitcoin.

b. I have also reviewed a publicly available profile of "Blake Benthall" on Twitter, another social networking website, which includes a photograph of BENTHALL as the user of the account, depicting the same individual associated with the GitHub account, discussed above. I have reviewed a post on that Twitter profile, dated on or about November 6, 2013, the date

when Silk Road 2.0 was publicly launched, stating: "All this talk about the #SilkRoad being back up makes me want to watch #ThePrincessBride."

43. I have also reviewed records from various sources reflecting that BLAKE BENTHALL, a/k/a "Defcon," the defendant, has had a steady stream of income in the form of Bitcoins since November 2013, when the Silk Road 2.0 website was launched. Specifically:

a. I have reviewed records provided by a U.S.-based Bitcoin exchanger ("Exchanger-1"), for an account registered under the name "Blake Benthall" and linked to Benthall Email Account-1 ("Bitcoin Account-1"). According to transaction records for Bitcoin Account-1, BENTHALL engaged in his first Bitcoin transaction with Exchanger-1 on or about November 7, 2013, the day after Silk Road 2.0 was publicly launched. The transactional records reflect that, since that date, BENTHALL has received a total of approximately 575.58 Bitcoins into the account through on or about October 28, 2014, and that BENTHALL has exchanged approximately 543.63 of those Bitcoins for United States currency, totaling $273,626.60.

b. I have reviewed emails from Benthall Email Account-1 reflecting numerous postings made by BENTHALL on a certain website that offers a service enabling users to post offers to buy or sell Bitcoins from other users of the site. The emails indicate that, from in or about November 2013, through in or about July 2014, BENTHALL sought to sell approximately $45,000 worth of Bitcoins over the site, and consummated sales totaling $25,000.

c. I have reviewed emails from Benthall Email Account-1 reflecting that BENTHALL purchased a luxury vehicle with Bitcoins in late January 2014 - approximately one month after Defcon assumed control of Silk Road 2.0. Specifically, email correspondence indicates that, in or about late January 2014, BENTHALL made a down payment of approximately $70,000 in Bitcoins towards the purchase of a Tesla Model S, worth approximately $127,000 in United States currency.

44. Further, the investigation has revealed that BLAKE BENTHALL, a/k/a "Defcon," the defendant, has used a combination of versions of software, matching the software used by Defcon to access the customer support interface of Silk Road 2.0. Specifically:

a. During the investigation, the HSI-UC has had access to the customer support interface for Silk Road 2.0, where administrators may log on to respond to requests for support from members and vendors on the website. Through the HSI-UC's access to the support interface, the HSI-UC has been able to observe the operating system and the web browser used by any administrator when accessing the support interface. On or about April 6, 2014, the HSI-UC observed that Defcon was logged into the support interface, and observed Defcon, to be using the Google Chrome web browser, version 35.0.1910.3 and a computer running the Apple OS X operating system, version 10.9.0, at the time.[11] Defcon is the only administrator whom the HSI-UC has observed log into the support interface with that browser and operating system combination.

b. Records provided by Exchanger-1 regarding Bitcoin Account-1 indicate that on the same date, BENTHALL logged into Bitcoin Account-1, using the identical combination of software: Google Chrome web browser version 35.0.1910.3 and the Apple OS X operating system, version 10.9.0.

c. According to publicly available information, on or about April 6, 2014, Google Chrome version 35.0.1910.3 was a beta version of the browser,[12] and Apple OS X version 10.9.0 was outdated.[13] Thus, based on my training and experience, this particular combination of software versions would not have been common among Internet users at the time.[14]

---

[11] The information available to the HSI-UC indicates that Defcon was not using Tor to access the customer support interface at the time, which would have caused Defcon's browser and operating system to appear differently.

[12] A "beta" version is a version of software that is released before the official version, to allow for a limited group of users, or sometimes the public at large, to test the product and provide feedback regarding bugs and other issues with the software.

[13] According to publicly available information, Apple OS X 10.9.0 had been outdated since December 16, 2013, having been replaced by two updated versions as of April 6, 2014.

[14] In addition to being able to observe Defcon's browser and operating system versions on the Silk Road 2.0 customer support interface, the HSI-UC was also able to observe Defcon's time zone via the Silk Road 2.0 interface, which regularly appeared

45. Physical surveillance of BLAKE BENTHALL, a/k/a "Defcon," the defendant, conducted in conjunction with online surveillance of Defcon on Silk Road 2.0 by the HSI-UC, further demonstrates that they are one and the same. Specifically, on September 10 and September 11, 2014, while BENTHALL was visiting relatives at their residence in Houston, Texas ("Residence-1"), FBI agents conducted physical surveillance of BENTHALL, while the HSI-UC simultaneously conducted online surveillance of Defcon on Silk Road 2.0. As set forth below, a comparison of the online surveillance with the physical surveillance reflects that BENTHALL was operating Defcon's account on Silk Road 2.0 at the time:

a. On or about September 10, 2014, at approximately 7:55 p.m. CDT, Defcon posted a public message to the SR2 Forum.

b. Approximately five minutes later, at approximately 8:00 p.m. CDT, Defcon's account on the SR2 Forum went inactive.

c. Shortly thereafter, at approximately 8:07 p.m. CDT, FBI agents observed BENTHALL depart Residence-1.

d. FBI agents maintained surveillance of BENTHALL and Residence-1, and observed that he did not return to Residence-1 until early the next morning, at approximately 3:36 a.m. CDT.

e. Based on observations made from the HSI-UC undercover administrative account, Defcon's account on the SR2 Forum remained inactive during the entire time that BENTHALL was gone from Residence-1.

f. Approximately three minutes after BENTHALL returned to Residence-1, at 3:39 a.m. CDT, Defcon's account on the SR2 Forum went active, and, at approximately 3:40 a.m. CDT, Defcon posted a message addressed to his staff.

46. A similar comparison of physical surveillance of BLAKE BENTHALL, a/k/a "Defcon," the defendant, with online surveillance of Defcon on Silk Road 2.0 on September 12, 2014,

---

as Pacific Daylight Time. This matches BENTHALL's time zone, as he is known to maintain his permanent residence in San Francisco, California.

further demonstrates that BENTHALL was in fact Defcon. Specifically:

a. On or about September 12, 2014, at approximately 8:06 p.m. CDT, FBI agents observed BENTHALL depart Residence-1.

b. According to Defcon's SR2 Forum profile, viewed through the HSI-UC's account at 8:36 p.m. CDT, Defcon was offline by that time, and his time of last activity was reported to be approximately 7:56 p.m. CDT, approximately ten minutes before BENTHALL was observed departing Residence-1.

c. At approximately 9:09 p.m. CDT, FBI agents observed BENTHALL return to Residence-1. Shortly after BENTHALL arrived, Defcon was observed to be back online on the SR2 Forum.

d. At approximately 9:17 p.m. CDT, FBI agents observed BENTHALL depart Residence-1. Defcon's status on the SR Forum thereafter remained as "active in past 30 minutes," until approximately 9:47 p.m. CDT, when Defcon's status was changed to "offline." According to the HSI-UC, this indicates that Defcon had stopped his online activity on the SR2 Forum approximately 30 minutes earlier - when BENTALL was observed leaving Residence-1 - as a user's status automatically changes to "offline" after 30 minutes of inactivity.

e. Accordingly, based on the foregoing, I believe that on or about September 12, 2014, BENTHALL accessed Silk Road 2.0 as Defcon from Residence-1 up until 7:56 p.m. CDT, and left Residence-1 approximately ten minutes later. He returned approximately an hour later, at approximately 9:09 p.m. CDT, and within ten minutes, quickly logged onto the SR2 Forum as Defcon. At approximately 9:17 p.m. CDT, BENTHALL left Residence-1, coinciding with Defcon ceasing activity on the SR2 Forum around the same time.

47. Finally, pen register data for an IP address associated with Residence-1 ("the Residence-1 IP Address") compared with surveillance of BLAKE BENTHALL, a/k/a "Defcon," the defendant, provides further confirmation that BENTHALL operated as Defcon on Silk Road 2.0. Specifically:

a. On or about September 12, 2014, pursuant to a judicial order issued the previous day, the FBI started collecting pen register data for the Residence-1 IP Address.

b. From on or about September 12, 2014 through on or about September 14, 2014, FBI agents observed BENTHALL repeatedly enter and exit Residence-1, and spend overnight hours at Residence-1. On or about September 14, 2014, at approximately 3:27 p.m. CDT, FBI agents observed BENTHALL depart Residence-1 with a suitcase. On or about September 15, 2014, at approximately 12:07 a.m. CDT, FBI agents observed BENTHALL arrive at his residence in San Francisco, California.

c. I have reviewed and analyzed pen register data for the Residence-1 IP Address, which reveals the transmission of a significant volume of Tor-related traffic to and from the Residence-1 IP Address from on or about the morning of September 12, 2014 through the approximate time on or about September 14, 2014 that BENTHALL departed Residence-1 to return to San Francisco. Since then, I have not observed any Tor-related traffic transmitted to or from the Residence-1 IP Address.

d. Based on my training and experience, and my familiarity with this investigation, I believe that the correlation of Tor-related traffic to BENTHALL's presence at Residence-1 further confirms BENTHALL's involvement in owning and operating Silk Road 2.0 as "Defcon."

WHEREFORE, I respectfully request that an arrest warrant be issued for BLAKE BENTHALL, a/k/a "Defcon," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

Vincent D. D'Agostino
Special Agent
Federal Bureau of Investigation

Sworn to before me this
29th day of October 2014

S/ Gabriel Gorenstein
HON. GABRIEL W. GORENSTEIN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

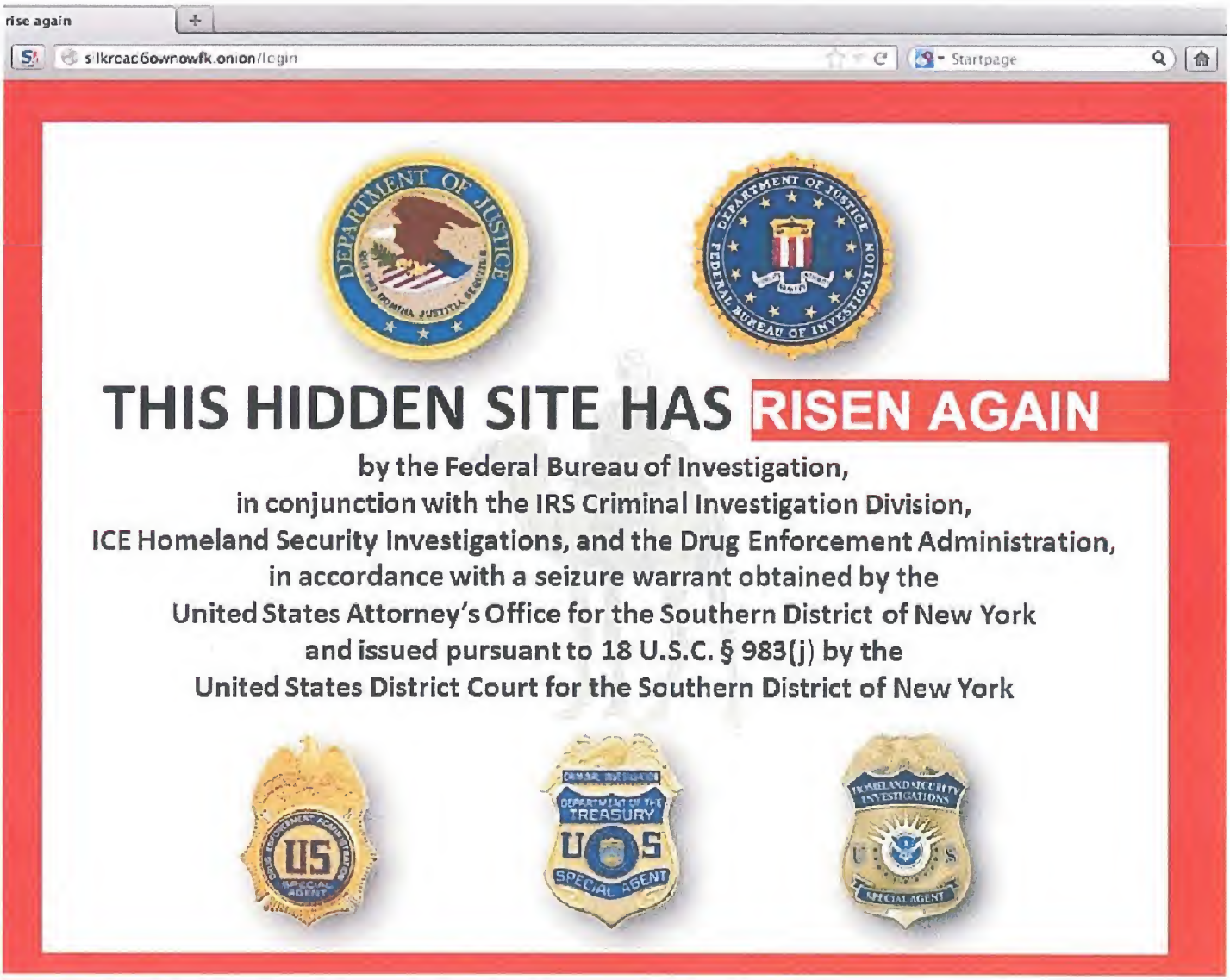
rise again
silkroad6ownowfk.onion/login
Startpage
DEPARTMENT OF JUSTICE
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
THIS HIDDEN SITE HAS RISEN AGAIN
by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York
US
SPECIAL AGENT
DEPARTMENT OF THE TREASURY
U S
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
SPECIAL AGENT

EXHIBIT A

ad

silkroad6ownowfk.onion/categories/drugs/items

Startpage

Silk Road

anonymous market

messages 0 | orders 0 | account B0.000

now accepting New Vendor Registrations

Search Go

Hi [redacted]

settings - logout

0

- Drugs *14024*
  - Stimulants *1801*
  - Psychedelics *1654*
  - Prescription *3644*
  - Precursors *29*
  - Other *472*
  - Opioids *360*
  - Ecstasy *1921*
  - Dissociatives *108*
  - Cannabis *1816*
  - Steroids/PEDs *1006*
- Alcohol *354*
- Apparel *543*
- Art *4*
- Books *176*
- Computer equipment *26*
- Custom Orders *85*
- Digital goods *348*
- Drug paraphernalia *192*
- Electronics *32*
- Erotica *55*
- Forgeries *112*
- Hardware *15*
- Herbs & Supplements *1*
- Jewelry *52*
- Lab Supplies *1*
- Lotteries & games *8*
- Medical *29*
- Money *138*
- Packaging *27*
- Services *121*
- Writing *7*

browsing drugs

sort by: bestselling ☐ ships to my region ☐ ships from my region update

1g Platinum Standard Pure Fire MDMA

B0.222831

★★★★★ (2452)

ships from: United States
ships to: United States

sold by Platinum Standard 95

5g White Widow

B0.157715

★★★★★ (1859)

ships from: Netherlands
ships to: Worldwide

sold by DutchMagic 92

Symbiosis - 1g MDMA - UK First Class

B0.099036

★★★★★ (1832)

ships from: United Kingdom
ships to: Worldwide

sold by Saint Symbiosis 93

1G of PURE UNCUT PERUVIAN COCAINE

B0.294664

★★★★★ (1903)

ships from: Germany
ships to: Worldwide

sold by fredthebaker 87

NY Heroin Stamp Bags (Very potent)

B0.048744

★★★★★ (1735)

ships from: United States
ships to: United States

sold by PCubeSensei 86

LIQUID MUSHROOMS [Pure Psilocybin] No Nausea, Faster Trip, Cleaner Feel Than Dried Shrooms (Click For Details)

B0.058803

★★★★★ (1493)

EXHIBIT B

Browser | AutoPlay | New Tab - Googl... | Silk Road - Tor Br...

ad

silkroad6ownowfk.onion/items/1g-3-afghan-heroin-high-quality-uncut-pure-from-the-brick-best-price-seller-on-all-markets

Startpage

Silk Road
anonymous market

messages 0 | orders 0 | account Ƀ0.000

now accepting
New Vendor Registrations

Search Go

Hi [redacted]
settings - logout

0

- Heroin *184*
  - Black tar *9*
  - Brown *79*
  - White *19*
- Alcohol *349*
- Apparel *532*
- Art *5*
- Books *279*
- Collectibles *2*
- Computer equipment *25*
- Custom Orders *92*
- Digital goods *360*
- Drug paraphernalia *196*
- Drugs *13362*
- Electronics *54*
- Erotica *55*
- Forgeries *189*
- Hardware *17*
- Herbs & Supplements *1*
- Jewelry *36*
- Lab Supplies *1*
- Lotteries & games *8*
- Medical *23*
- Money *158*
- Packaging *30*
- Services *123*
- Writing *7*

1g #3 Afghan Heroin High Quality Uncut Pure From The Brick Best Price Seller On All Markets

★★★★★ (68)

Ƀ0.123473

vendor: Baron Van H 86

ships from: Undeclared
ships to: Worldwide

Here You Can Buy Direct From The Source
My Rules Are Easy
Read My Profile !!

shipping options

description	est. delivery	shipping price	
International Air Post (0% Refund/Reship)	14 days	Ƀ0.017639	add to cart
International Post Trackable (100% Refund/Reship)	14 days	Ƀ0.052917	add to cart

more images

EXHIBIT C

Browser | Silk Road - Tor Br...